

# 修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院 電気通信学研究科 人間コミュニケーション学専攻 博士前期課程		
氏 名	志村 正法	学籍番号	0836008
論 文 題 目	安全で機能制限のない秘密分散データベースの研究		
<p>要 旨</p> <p>個人情報電子化されネットワーク上で授受されるに従い、その漏洩が社会問題となっている。個人情報の漏洩には様々な形態があるが、なかでもデータベースからの漏洩は大量の個人情報が一度に漏洩するので、極めて甚大な被害をもたらす。よって個人情報漏洩を防ぐため、データベースのセキュリティが重要である。</p> <p>データベースのセキュリティとして、データを暗号化して保護する方式が注目されている。しかし、従来のデータベース暗号化方式ではデータを保護することはできるが、データベースにおける演算が制限されてしまう。しかしデータベースの目的はデータの検索など様々な演算を可能にし、データを有効活用する事である。したがってデータベースが保護された状態を維持しつつ、任意の演算を可能にすることを研究の目的とした。</p> <p>まず、従来のデータベース保護技術を分析し、問題点を明らかにした。本研究では、関係データベースの任意の演算が関係代数によってモデル化されることに着目した。秘密分散されたデータベースにおいて、マルチパーティプロトコルを用いて関係代数を実行可能な方式を提案した。それによってデータベースが保護された状態を維持しつつ、任意の演算が可能となることを示した。</p>			